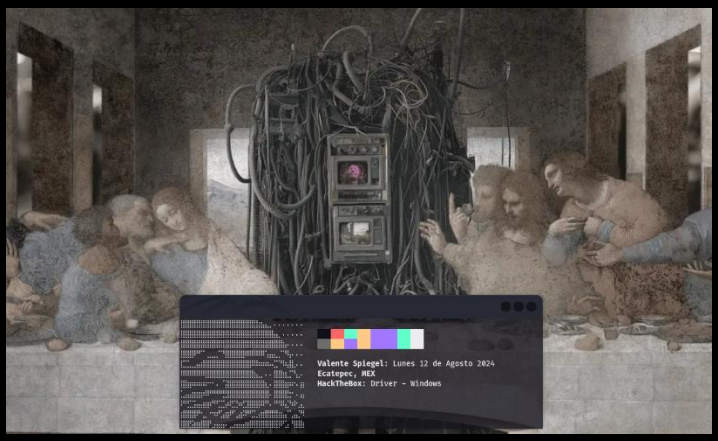
Ethical hacking lab : Driver HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

/▲\ Correo /▲\ tiktok /▲\ github

Atacante ---------- |10.10.19.30|
|>/////////// Linux|

Victima ---- ----------|10.10.11.130|
|> /////// Windows|



Walkthrough

| 1 | Al realizar una enumeración de puertos y servicios, se identificó un servicio web activo
| | el puerto 80, junto con SMB en el puerto 445 y WinRM en el puerto 5985. El sitio web
| | Protegido por autenticación HTTP básica. Es vulnerable a un ataque de Password Guessing, la
| | combinación admin:admin es aceptada, otorgando acceso al servicio.

| 2 | En el sitio web, se observó una función para cargar firmwares de impresora en el recurso
| | compartido SMB. Creé y subí un archivo malicioso SCF utilizando msfvenom, lo que resulto
| | en la captura del hash NTLM del usuario tony. Este hash fue descifrado con
| | John the Ripper, revelando la contraseña en texto plano y permitiendo iniciar sesión como
| | tony a través de winrm.

| 3 | Ya como tony, descubrí que la máquina era vulnerable a una explotación de privilegios
| | locales asociada con un controlador de impresora. Utilizando el exploit para Print
| | Spooler Local Privilege Escalation (PrintNightmare) [CVE-2021-1675],
| | logré elevar los privilegios a NT AUTHORITY\SYS

Habilidades.

>- Password Guessing

En un entorno donde las contraseñas son predecibles, Password Guessing puede ser una técnica manual efectiva y rápida para obtener acceso no autorizado intentando adivinar las credenciales de usuario mediante la prueba de combinaciones comunes de usernames y paswords "admin/admin"

>- SCF Malicious file

Los archivos (Shell Command File). Se utilizan principalmente para ejecutar comandos en Windows, como mostrar el escritorio o realizar otras tareas del sistema. En este caso uno malicioso especialmente diseñado para el robo del hash NTLM Windows mediante el abuso de la funcionalidad de los archivos.

>- CVE-2021-1675

La vulnerabilidad reside en el servicio de cola de impresión de Windows gestiona las operaciones de archivos y permisos. Un atacante que explote exitosamente esta vulnerabilidad podría ejecutar código arbitrario con privilegios elevados en un sistema vulnerable. Esto significa que el atacante podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con derechos completos de usuario.

Afecta: Todas las versiones soportadas de Windows en el momento en que se descubrió.
Tipo de Vulnerabilidad: Ejecución remota de código y escalación de privilegios.
Gravedad: Crítica.